Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Previously Presented) A method of establishing a secure communication link between a smart card and a central computer system through a communication network, the method comprising the steps of:

receiving at a smart card communication device an outgoing secure radio frequency signal transmitted from the smart card, the secure radio frequency signal including secured data formatted by the smart card to allow the central computer system to detect a modification to the secured data occurring during transmission beginning at the smart card and extending to the central computer system;

demodulating the outgoing secure radio frequency signal using the smart card communication device to produce an outgoing secure data signal, wherein the demodulating of the outgoing secure radio frequency signal is without deciphering the secured data;

formatting the outgoing secure data signal in accordance with a communication network protocol to produce an outgoing formatted secure signal; and

transmitting the outgoing formatted secure signal to the central computer system, wherein the central computer system is remote from the smart card communication device and is configured to detect the modification to the secured data and to process a transaction for the smart card using the secured data included in the outgoing formatted secure signal.

2. (Original) A method in accordance with claim 1 further comprising the step of subjecting outgoing secure data contained within the outgoing secure radio frequency signal to a security function only at the smart card and at the central computer system.

3. (Canceled)

4. (Previously Presented) A method in accordance with claim 1 further comprising the steps of:

reformatting, at the central computer system, the outgoing formatted secure signal to produce the outgoing secure data signal, the outgoing secure data signal comprising the secured data; and

decoding, at the central computer system, the outgoing secure data signal to receive smart card information included within the outgoing secure data signal.

5. (Previously Presented) A method in accordance with claim 4 further comprising the steps of:

receiving an incoming secure formatted signal from the central computer system at the smart card communication device through the communication network, the incoming secure formatted signal formatted in accordance with the communication network protocol;

reformatting the incoming secure formatted signal using the smart card communication device to produce an incoming secure data signal; and

transmitting an incoming secure radio frequency signal from the smart card communication device to the smart card, wherein the incoming secure radio frequency signal is modulated in accordance with the incoming secure data signal.

6. (Original) A method in accordance with claim 5 further comprising the steps of:

demodulating the incoming secure radio frequency signal within the smart card to produce the incoming secure data signal; and

decoding the incoming secure data signal to receive central computer information included within the incoming secure data signal.

7. (Previously presented) A method in accordance with claim 6 wherein the step of decoding the outgoing secure data signal comprises the step of implementing a security function using a security device remote from the smart card communication device and coupled to the central computer system to decode the outgoing secure data signal.

8. (Original) A method in accordance with claim 7 further comprising the step of encoding outgoing data within the smart card using a security function to produce the outgoing secure data signal.

9. (Original) A method in accordance with claim 8 wherein the step of encoding further comprises the steps of:

generating a message authentication code at the smart card; and

appending the message authentication code to the outgoing data.

10. (Original) A method in accordance with claim 9, wherein the step of decoding comprises the step of observing a characteristic of the outgoing data in accordance with the message authentication code.

11. (Previously Presented) A method in accordance with claim 10, wherein the step of observing comprises the step of:

generating the message authentication code at the central computer system; and

comparing the secure outgoing data signal to the message authentication code to detect the modification to the secured data.

12. (Original) A method in accordance with claim 10 wherein the step of decoding the incoming secure data signal comprises the step of decoding the incoming secure data signal within the smart card using a security function.

13. (Original) A method in accordance with claim 7 further comprising the step of encoding incoming data within the central computer system using a security function to produce the incoming secure data signal.

14. (Original) A method in accordance with claim 13 wherein the step of encoding further comprises the steps of:

generating a message authentication code at the central computer system; and

appending the message authentication code to the incoming data.

15. (Previously presented) A method in accordance with claim 14, wherein the step of decoding the incoming secure data signal comprises the step of observing a characteristic of the incoming secure data signal in accordance with the message authentication code.

16. (Original) A method in accordance with claim 15, wherein the step of observing comprises the step of:

generating the message authentication code at the smart card; and

comparing the secure incoming data signal to the message authentication code to detect an unauthorized modification of the incoming data.

17. (Previously Presented) A method of establishing a secure communication link between a smart card and a central computer system through a communication network, the method comprising the steps of:

encoding, using the smart card, information within the smart card using a security function to produce an outgoing secure data signal comprising a first set of secured data, the first set formatted to allow the central computer system to detect a modification to the first set occurring during transmission beginning at the smart card and extending to the central computer system;

transmitting an outgoing secure radio frequency signal including the outgoing secure data signal to a smart card communication device;

demodulating an outgoing secure radio frequency signal at the smart card communication device to produce the outgoing secure data signal;

formatting the outgoing secure data signal in accordance with a communication network protocol to produce an outgoing formatted secure signal;

transmitting the outgoing formatted secure signal to the central computer system through a communication network, the central computer system located remotely from the smart card communication device;

reformatting the outgoing formatted secure signal to produce the outgoing secure data signal; and

decoding, using a security device coupled to the central computer system, the outgoing secure data signal to receive the smart card information and to detect whether the modification to the first set occurred during transmission beginning at the smart card and extending to the central computer system;

processing, using the central computer system, a transaction for the smart card using the decoded smart card information;

encoding central computer system information using the security device to produce an incoming secure data signal comprising a second set of secured data, the second set formatted to allow the smart card to detect a modification to the second set occurring during transmission beginning at the central computer system and extending to the smart card;

formatting the incoming secure data signal to produce an incoming secure formatted signal;

receiving the incoming secure formatted signal from the central computer system through the communication network, the incoming secure formatted signal formatted in accordance with the communication network protocol;

reformatting the incoming secure formatted signal to produce the incoming secure data signal; and

transmitting an incoming secure radio frequency signal to the smart card, wherein the incoming secure radio frequency signal is modulated in accordance with the incoming secure data signal;

demodulating the incoming secure radio frequency signal within the smart card to produce the incoming secure data signal; and

decoding the incoming secure data signal using a security function within the smart card to receive the central computer information at the smart card and to detect whether the modification to the second set occurred during transmission beginning at the central computer system and extending to the smart card.

18. (Previously Presented) A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

exchanging secure data through a radio frequency communication channel from a smart card communication device to the smart card;

exchanging the secure data through a communication network from the central computer system to the smart card communication device;

performing a security function at the smart card on the secure data received from and generated at the central computer system to detect whether a modification to the secure data occurred during transmission beginning at the central computer system and extending to the smart card;

performing the security function on the secure data at the central computer system to format the secure data to allow the smart card to detect a modification to the secure data occurring during transmission beginning at the central computer system and extending to the smart card; and

processing, using the central computer system, a transaction for the smart card using the secure data.

19. (Canceled)

20. (Original) A method in accordance with claim 18 wherein the step of exchanging the secure data through the communication network comprises the steps of:

formatting secure data in accordance with a communication network protocol;

transmitting the secure data through the communication network;

and reformatting the secure data.

21. (Previously Presented) A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

downloading communication link interface software to a processor local to a smart card communication device from a HTTP server in a remote computer system;

exchanging secure data between the smart card and the smart card communication device through a radio frequency communication channel, the secure data formatted by the smart card to allow the central computer system to detect a modification to the secure data occurring during transmission beginning at the smart card and extending to the central computer system;

exchanging the secure data between the smart card communication device and the central computer system through the processor running the downloaded communication link interface software, wherein the processor is coupled to the central computer system through a communication network and the processor is located remotely from the central computer system; and

processing, using the central computer system, a transaction for the smart card using the secure data.

22. (Previously Presented) A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card communication device, the method comprising the steps of:

exchanging secure data with a smart card communication device through a baseband data channel, wherein the secure data comprises data exchanged between the smart card communication device and the smart card through a radio frequency channel;

formatting the secure data at the smart card communication device in accordance with a communication network protocol;

exchanging the secure data between the smart card communication device and the central computer system through a communication network, wherein the secure data is formatted by the smart card to allow the central computer system to detect a modification to the secure data occurring during transmission beginning at the smart card and extending to the central computer system; and

processing, using the central computer system, a transaction for the smart card using the secure data.

23. (Original) A method in accordance with claim 22 wherein the secure data is not deciphered within the communication link.

24. (Original) A method in accordance with claim 22 further comprising the step of subjecting the secure data to a security function only at the smart card and at the central computer system.

25. (Previously Presented) A smart card communication system for establishing a secure communication link between a smart card and a central computer system, the smart card communication system comprising:

a smart card communication device comprising a radio frequency transceiver adapted to exchange secure data with the smart card through a radio frequency communication channel and a data communication interface;

a processor coupled to the smart card communication device, the processor adapted to exchange the secure data with the data communication interface through a baseband data channel;

a communication network coupled to the processor and adapted to exchange the secure data in accordance with a communication network protocol between the processor and the central computer system located remotely from the processor;

a security device coupled to the central computer system and configured to format the secure data to allow the smart card to detect a modification to the secure data occurring during transmission beginning at the central computer system and extending to the smart card, the security device located remotely from the processor; and

a smart card adapted to receive the secure data and detect whether a modification to the secure data occurred during transmission beginning at the central computer system and extending to the smart card.

26. (Original) A system in accordance with claim 25 wherein the communication network is an Internet network and the communication network protocol is an Internet protocol.

27. (Original) A system in accordance with claim 25 further comprising a smart card adapted to subject outgoing data to a security function to produce a secure outgoing data signal.

28. (Canceled)

29. (Previously Presented) A smart card communication device for interfacing within a smart card communication system having a local processor coupled to a remotely located central computer system through a communication network, the smart card communication device comprising:

a radio frequency transceiver adapted to exchange secure data with a smart card through a radio frequency communication channel, the secure data formatted by the smart card to allow the central computer system to detect a modification to the secure data occurring during transmission beginning at the smart card and extending to the central computer system;

a data communication interface adapted to exchange the secure data with the processor through a baseband data communication channel without deciphering the secure data.

30. (Original) A device in accordance with claim 29 wherein the transceiver comprises:

a receiver adapted to receiving a secure outgoing radio frequency signal from a smart card to produce a secure outgoing data signal, the data communication interface adapted to send the outgoing data signal through the baseband data channel in a secure state.

31. (Original) A device in accordance with claim 30 wherein the receiver comprises a demodulator adapted to demodulate the secure outgoing radio frequency signal to produce the secure outgoing data signal, the secure outgoing data signal comprising a plurality of logic highs and a plurality of logic lows corresponding to an intelligible message only when subjected to a security function.

32. (Original) A device in accordance with claim 30 wherein the receiver comprises a demodulator adapted to demodulate the secure outgoing radio frequency signal to

produce the secure outgoing data signal, the secure outgoing data signal comprising a plurality of logic highs and a plurality of logic lows corresponding to a verifiable authentic message only when subjected to a security function.

33. (Original) A device in accordance with claim 29 wherein the transceiver comprises a transmitter adapted to transmit a secure incoming radio frequency signal to the smart card, the secure incoming radio frequency signal based on a secure incoming data signal received by the data communication interface.

34. (Original) A device in accordance with claim 33, wherein the transmitter comprises a modulator adapted to modulate the secure incoming data signal to produce the secure incoming radio frequency signal, the secure incoming data signal comprising a plurality of logic highs and plurality of logic lows corresponding to an intelligible message when subjected to a security function.

35. (Original) A device in accordance with claim 33, wherein the transmitter comprises a modulator adapted to modulate the secure incoming data signal to produce the secure incoming radio frequency signal, the secure incoming data signal comprising a plurality of logic highs and plurality of logic lows corresponding to a verifiable authentic message only when subjected to a security function.

36-58. (Canceled)

59. (Previously Presented) A method in accordance with claim 1 wherein the secured data is formatted to allow the central computer system to authenticate identity of the sender.